UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/014,763	12/11/2001	Juan A. Garay	8-32	6594

7590 11/23/2005

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER	
LEMMA, SAMSON B	
ART UNIT	**PAPER NUMBER**
2132	

DATE MAILED: 11/23/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 10/014,763	**Applicant(s)** GARAY ET AL.	
	Examiner Samson B. Lemma	**Art Unit** 2132	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 September 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. This office action is in reply to an amendment filed on September 09, 2005. **Claims 2-3** have been amended, **and claims 1-25** are pending.

Response to Arguments

2. Applicant's argument filed on September 09, 2005 have been fully considered but they are not persuasive.

The first argument by the applicant is with regard to a 102 (e) rejection made to the independent claims 1 and 22-25. Applicant argued that independent claims include limitations that are not shown or suggested by the references on the record, namely **Aura. Applicant wrote the following in support of his argument,** "With this statement, the Examiner apparently argues that element 406 in Aura's FIG. 4 is analogous to the verifier element in claim 1 , element 407 is analogous to the "intermediary device" element, and element 409 describes the returned to the verifier of a second digital signature generated by the intermediary device. Applicants respectfully disagree. Claim 1 requires, in part, that the intermediary device check that the first digital signature is a valid digital signature for the user and if the first digital signature is valid" generate a second digital signature which is returned to the verifier as a signature generated by the user device." Assuming, as the Examiner does, that the intermediary device is represented by element 407 and the verifier is represented by element 406,

this would mean that Aura's figure would have to show a second digital signature going from element 407 to element 406 if that figure were to show a technique identical to that in claim 1.

However, careful examination of FIG. 4 shows that neither element 407, nor 409, has an output terminating in element 406. In fact, element 406 only has one input, that originating in element 405 which the Examiner argues represents a first digital signature. As a result, Aura's FIG. 4 is not functionally identical to the technique described in claim 1, and Aura does not anticipate claim 1 under 102(e)."

Examiner disagrees with this argument.

The Examiner disagreement is based on the fact that the element/entity shown on figure 4, ref. Num "406" and "409" are not two different entities as applicant argued rather these two entities are actually one and the same entity and are VPLMN (visited public land mobile network) which is met the verifier.

Examiner would point that Aura on page 10, lines 1-3 discloses the following facts in support of his argument.

The center sends the generated random number RAND2 and the results SRES1, SRES2' and Kc of the hash functions **to the network VPLMN.**" Furthermore on page 11, lines 3-6, Aura teaches the fact that **the same said VPLMN** receives SRES2 from the mobile station and compares it to the value **SRES2' it has received from the center.**

Therefore Aura clearly discloses as shown above the fact that the element/entity shown on figure 4, ref. Num "406" and "409" are not two different entities as applicant argued rather these two entities are actually one and the same entity and they are VPLMN (visited public land mobile network) which is met the verifier.

By the same analogy, element/entity shown on 4, ref. Num "407" and "408" are not two different entity as applicant argued, rather they are one and the same entity which are the mobile station.

Aura discloses the following in support of this remark.

Aura on page 10, line 6, and on figure 4, ref. Num "406 & 407" discloses the fact that the mobile station/which is met to be "intermediary device" receives the values RAND2 and SRES1/first digital signature from the **VPLMN/verifier. Furthermore the Aura on page on page 10, lines 17-19 discloses that the same mobile station which is met to be intermediary device checks the validity of the first digital signature by comparing the first digital signature SRES1 to the values SRES1' it has generated itself.**

Like wise, Aura on page 20-21, discloses the fact that after successful identification, the same mobile station sends the generated SRES2/second digital signature to the verifier/ network VPLMN.

Therefore applicant argument recited as "**neither element 407, nor 409, has an output terminating in element 406 is wrong. And the other argument presented by the applicant as "in fact, element 406 only has one input, that originating in element 405" is also wrong because as stated above "406" and "409" are actually one and the same element/entity which is VPLMN (visited public land mobile network) which is met the verifier and by the same token, elements "407" and "408" are not two different entities/elements but they are one and the same element which is mobile station which is met the intermediary device.**

Therefore examiner asserts that the rejection is valid and clarifies the rejection as follows to show how the each and every limitation of the independent claims **is anticipated by Aura.**

Aura discloses

- **Generating in the user device a first digital signature**; [Figure 4, reference "405" and ref. Num "SRES1";page 10, lines 1-3**)** (As disclosed on page 10, lines 1-3 and shown on figure 4, ref. Num "405", first digital signature "SRES1" is generated)

- **Sending the first digital signature to the verifier;** [figure 4, ref. Num "406", "SRES1"; page 10, lines 1-3](As discloses on page 10, lines 1-3 and shown on figure "406" and "405"; the first digital signature SRES1 is sent to the VPLMN which is met the verifier.)

- **Wherein the verifier sends the first digital signature to the intermediary device,** [figure 4, ref. Num "407" and ref. Num "SRES1" and page 10, line 6,] (the verifier which is met the VPLMN shown on figure 4, ref. Num "406" sends a first digital signature **"SRES1"** to the intermediary device which is met the "mobile station" shown on figure 4, ref. Num "407") and

- **The intermediary device checks that the first digital signature is a valid digital signature for the user device** [figure 4, ref. Num "408"; page 10, lines 17-20](Aura on page on page 10, lines 17-20 discloses that the same mobile station which is met to be intermediary device checks the validity of the first digital signature by comparing the first digital signature SRES1 to the values SRES1' it has generated itself**) and .**

- **If the first digital signature is valid [figure 4, ref. Num "408", "Yes"] generates a second digital signature** [figure 4, ref. Num "407 & 408", "SRES2"] **which is returned to the verifier (**figure 4, ref. Num "SRES2", "409"**) as a signature generated by the user device** [Figure 4, ref. "SRES2" and Num "408"]. (Aura on page on page 10, lines 17-20 discloses that the same mobile station which is met to be intermediary device checks the validity of the first digital signature by comparing the first digital signature SRES1 to the values SRES1' it has generated itself. Aura on page 20-21, further discloses the fact that after successful identification or if the first digital signature is found valid, the same mobile station sends the generated SRES2/second digital signature to the same/said verifier/ network VPLMN.)

Applicant's second argument is regarding the dependent claims.

Applicants argued that since the independent claims are patentable therefore all the claims dependent thereon are also in condition for allowance for the same reasons argued for the independent claims.

In response to the above argument by the applicant, the examiner response discussed to the independent claims above is also valid towards this argument. Therefore all the elements of the limitations is suggested and disclosed by primary reference/s on the records and the rejection remains valid.

3. The 35 USC § 112 rejection given to claims 2 and 3 by the former office action is still kept. Applicant's amendment made to claims 2 and 3 does not over come the rejection successfully.

Claim Rejections - 35 USC § 112

4. The following is a quotation of the second paragraph of 35 U.S.C 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

5. **Claim 2** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 2 recite the limitation "**having a computational efficiency compatible with computational resources of the user device**". This term is not only vague but also not clear. The claim has to be rewritten so

that there would not be any ambiguity. For the purpose of examination the limitation is taken out from the respective claim.

6. **Claim 3** is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Claim 3 recite the limitation "...**having a computational efficiency lower than that of the first digital signature protocol.** " This term is not only vague but also not clear. The claim has to be rewritten so that there would not be any ambiguity. For the purpose of examination the limitation is taken out from the respective claim.

7. **Claims 4-8** depend from rejected claim 2 and 3, and include all the limitations of the respective claim, thereby rendering those dependent claims indefinite.

Claim Rejections - 35 USC § 102

8. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

9. **Claims 1-7,9-10,17, 19-25** are rejected under 35 U.S.C. 102(e) as being anticipated by **Aura**. (hereinafter referred to as **Aura**) (U.S. Patent No. 6,711,400 B1).

10. **As per claim 1 and 22-25**

Aura discloses a method for use in generating digital signatures in an information processing system, the system including at least a user device, an intermediary device and a verifier, the method comprising the steps of:

- **Generating in the user device a first digital signature**; [Figure 4, reference "405" and ref. Num "SRES1";page 10, lines 1-3**)** (As disclosed on page 10, lines 1-3 and shown on figure 4, ref. Num "405", first digital signature "SRES1" is generated)

- **Sending the first digital signature to the verifier;** [figure 4, ref. Num "406"; page 10, lines 1-3](As discloses on page 10, lines 1-3 and shown on figure "406" and "405"; the first digital signature SRES1 is sent to the VPLMN which is met the verifier.)
- **Wherein the verifier sends the first digital signature to the intermediary device,** [figure 4, ref. Num "407" and ref. Num "SRES1" and page 10, line 6,] (the verifier which is met the VPLMN shown on figure 4, ref. Num "406" sends a first digital signature **"SRES1"** to the intermediary device which is met the "mobile station" shown on figure 4, ref. Num "407") and
- **The intermediary device checks that the first digital signature is a valid digital signature for the user device** [figure 4, ref. Num "408"; page 10, lines 17-20](Aura on page on page 10, lines 17-20 discloses that the same mobile station which is met to be intermediary device checks the validity of the first digital signature by comparing the first digital signature SRES1 to the values SRES1' it has generated itself**) and .**

- **If the first digital signature is valid [figure 4, ref. Num "408", "Yes"] generates a second digital signature** [figure 4, ref. Num "407 & 408" and "SRES2"] **which is returned to the verifier** (figure 4, ref. Num "SRES2", "409") **as a signature generated by the user device** [Figure 4, ref. "SRES2" and Num "408"]. (Aura on page on page 10, lines 17-20 discloses that the same mobile station which is met to be intermediary device checks the validity of the first digital signature by comparing the first digital signature SRES1 to the values SRES1' it has generated itself. Aura on page 20-21, further discloses the fact that after successful identification or if the first digital signature is found valid, the same mobile station sends the generated SRES2/second digital signature to the same/said verifier/ network VPLMN.)

11. **As per claim 2, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore Aura discloses the method wherein the first digital signature is generated using a first secret key. [See figure 4, ref. Num "405" and secret Key "Ki" and "SRES1"]

12. **As per claim 3, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore Aura discloses the method wherein the second digital signature is generated using a second secret key [See figure 4, ref. Num "407" and secret key "KI" and "SRES2"]

13. **As per claim 4 and 5, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore Aura discloses the method wherein an agreement relating to corresponding public keys of the first and second digital signature protocols is signed

by both the user device and the intermediary device and the resulting twice-signed agreement is stored by both the user device and the intermediary device. [Figure 4]

14. **As per claim 6, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore Aura discloses the method wherein **the first digital signature comprises a signature s1 on a message m,** [figure 4, ref. 405 and "SRES1"] the **signature s1 being generated using a secret key s'** [figure 4, ref. Num "405" and "Ki"] **associated with the user device**. [figure 4]

15. **As per claim 7, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore **Aura discloses the method wherein the first digital signature comprises a signature s1 on h(m),** [figure 4, ref. Num "405" See H1] **where m is a message and h is a hash function, the signature s1 being generated using a secret key s'** [figure 4, ref. Num "405" and "Ki"] **associated with the user device.** [figure 4]

16. **As per claim 9, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore **Aura discloses the method wherein the second digital signature comprises a signature s2 on a message m,** [figure 4, ref. Num "SRES2"] **the signature s2 being generated using a secret key s** [figure 4, ref. Num "407" See KI] of **associated with the user device. [figure 4]**

17. **As per claim 10, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore **Aura discloses the method wherein the second digital signature comprises a signature s2** [figure 4, ref. Num "407", "SRES2"] **on h(m), where m is a message and h is a hash function,** [Figure 4, ref. Num "407" and H2] **the signature**

s2 being generated using a secret key s [figure 4, ref. Num "407" See KI] of **associated with the user device. [figure 4]**

18. **As per claim 17, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore **Aura discloses the method wherein** the intermediary device is configured to wait a predetermined delay period between checking that the first digital signature is a valid signature and generating the second digital signature which is returned to the verifier. [Figure 4, ref. Num "408"]

19. **As per claim 19-21, Aura discloses** a method for use in generating digital signatures in an information processing system as applied to claim 1 above. Furthermore **Aura discloses the method wherein** the user device comprises a mobile telephone.[figure 1]

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. **Claims 8,11-16,18** are rejected under 35 U.S.C. 103(a) as being unpatentable **Aura**. (hereinafter referred to as **Aura**) (U.S. Patent No. 6,711,400 B1).

in view of **Micali et al**, (hereinafter referred to as **Micali**) (U.S. Patent No. 5,016,274)

22. **As per claim 8,11-16 and 18** **Aura** discloses verifier upon receipt of the first digital signature checks that the first digital signature is a valid digital signature using [Figure 4, ref. Num "409"]

Aura does not explicitly disclose that verifier upon receipt of the first digital signature checks that the first digital signature is a valid digital signature **using a first public key corresponding to the first secret key.**

However, in the same field of endeavor, **Micali** discloses that verifier upon receipt of the first digital signature checks that the first digital signature is a valid digital signature **using a first public key corresponding to the first secret key. [Figure 1, ref. Num "34"]**

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of verification digitat signature using the public key as per teaching of Micali in to the method verification as taught by **Aura**, in order to enhances the security and efficiency of known signature schemes.[See Micali Column 1, lines 7-9]

Conclusion

23. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA
S.L.
11/14/2005

GILBERTO BARRON Jr.
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100